



**ARCHBISHOP OF YORK'S CE JUNIOR SCHOOL**  
**ONLINE SAFETY (FORMERLY E-SAFETY) POLICY**

Date Adopted <b>July 2020</b>	<b>Jonathan Green</b> <b>Headteacher</b>	Signature 
Date for review <b>July 2023</b>	<b>Fiona Philips</b> <b>Chair of Governors</b>	Signature 



## **1.0 INTRODUCTION**

We are a welcoming, inclusive family with a strong Christian ethos. We continually aim to be an excellent school where people care more than others think is wise, risk more than others think is safe, dream more than others think is practical and expect more than others think is possible.

## **2.0 BACKGROUND AND LINKED POLICES**

Archbishop of York's C.E. Junior School (AYJS) has a duty to provide pupils and staff with access to quality learning using internet technologies and electronic communications and, with this, the responsibility to ensure that this learning takes place safely.

Together with the Computing policy (Ref: PC\_4.4), the Online Safety policy recognises our commitment to online safety and acknowledges its part in the school's overall safeguarding policies and procedures. It operates in conjunction with other policies including but not limited to those for:

- Pupil Behaviour (Ref: PC\_1.2),
- Anti-Bullying (Ref: PC\_1.4),
- Information Security (Ref: GEN\_4.3),
- Safeguarding and Child Protection (Ref: GEN\_2.0)
- ICT Acceptable Use – Pupils (Ref PC\_1.7) and
- ICT Acceptable Use – Staff (Ref: SPF\_1.7).

## **3.0 AIMS TO BENEFIT EDUCATION AND ENHANCE LEARNING**

- Access to educational resources and to experts in many fields for pupils and staff.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Professional development for staff through access to national standards, educational materials and effective curriculum practice.
- Improved access to technical support including remote management of Networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority and the DFE.
- Access to learning wherever and whenever convenient.
- The school internet access will be designed for pupil use to include filtering appropriate to the age of the pupils.
- Pupils will be taught acceptable, effective and safe use of the internet and access will be planned to enrich and extend learning activities.

## **4.0 GUIDLINES**

### **4.1 Managing Internet Access**

- Pupils at AYJS do not have access to personal external E-mail and only have access to the internet via a responsible adult.
- Clear objectives will be taught to pupils regarding acceptable use of the Internet.
- Pupils will be taught about the risk of Online (Cyber) Bullying and how to avoid it.
- Pupils will be taught the dangers of social network sites outside of school.

- The appropriate use of the G-Suite tools will be taught and pupils will be expected to conform to appropriate standards of behaviour.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Parents' attention will be drawn to the school's Online Safety Policy in newsletters, the school prospectus and on the school Website.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- Photographs that include pupils will be selected carefully for use on the Website.
- Pupils' names will not be used on the Web site in association with photographs.
- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- All staff must read and sign the 'Staff Acceptable Use Agreement' before using any school ICT resource.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential at all times.
- The sending of abusive or inappropriate text messages, emails, files by Bluetooth or any other means is forbidden.
- Staff and pupils must understand that if they see an unacceptable image on a computer screen, turn off the screen, and then report immediately to the Local Authority helpdesk via the I.C.T. coordinator or Headteacher.
- AYJS will ensure that staff are aware they must not use Internet copyright material without permission.
- The school will work in partnership with the Local Authority, the South York MAT, the Department for Education, Vital York Ltd, the school's ICT support provider, and the Internet Service Provider to ensure filtering systems are as effective as possible.
- School ICT systems capacity and security will be reviewed regularly and reviewed with the Local Authority, the South York MAT and Vital York Ltd.
- The school will develop further guidance if the school's network and I.T. equipment has a community use.

#### **4.2 E-mail**

- Pupils can only use the Gmail account assigned to their Google account provided by Vital York Ltd. They cannot access personal accounts whilst at school.
- Pupils will be taught acceptable use of their email accounts. All emails sent and received are filtered for language use and this is overseen by Vital York Ltd. Teachers do have access to passwords and will access a child's account if we feel this is a necessary step to ensure appropriate use is occurring.
- Pupils will be reminded not to reveal personal information about themselves or others without specific permission.
- Access in school to external personal e-mail accounts will be allowed for staff only.
- E-mail sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper.
- All school related e-mails must be sent from the school's secure and encrypted email system.
- To comply with GDPR if e-mails are to be sent to multiple recipients the blind copy (Bcc) facility should be used.
- The forwarding of chain letters is not permitted.

### **4.3 Emerging Technologies**

- Mobile phones are not allowed to be used in school by pupils unless permission from a staff member is given.
- Staff should refrain from using their mobile phones for personal reasons within lessons.
- If photographs are to be taken on a personal device for school approved social media accounts, the staff member must delete the photos immediately after uploading.
- Staff must ensure their device is secured with a pin, pattern or facial recognition software.
- Staff should try to log in to their school email account before lessons start so that their mobile phone should not be needed for the verification purpose during a lesson.
- Staff will be encouraged to use a school phone where contact with pupils or a parent is required.
- Gaming technology such as Sony PlayStation and Microsoft Xbox which allows Internet access may not include filtering so will not be allowed in school without adult supervision.
- Access to wireless internet connection requires Head teacher permission.

### **4.4 Social Networking**

The school recognises that many staff will actively use Facebook, Twitter and other such social networking, blogging and messaging services. It is recognised that some such services may have an appropriate application in school, however, where such activities are planned, a separate account should be set up for the purpose and there should be no connection made between personal and school accounts used for educational purposes. Any such accounts and activities should be approved by a member of the SLT prior to use.

It is likely that approved school social media accounts will be accessed during the school day. Staff must ensure that this is done at appropriate times. Staff must also be aware of the media list and ensure that parent permission has been given before posting a photograph or video of a child.

Personal social media accounts should only be accessed by staff in their own time. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via their personal accounts. Staff are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.